PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

WO 89/1286

(51) International Patent Classification 4 : **G06F 12/14, 13/00**	**A1**	**(11) International Publication Number:** **WO 89/1286** **(43) International Publication Date:** 28 December 1989 (28.12.8

(21) International Application Number: PCT/US89/02360

(22) International Filing Date: 2 June 1989 (02.06.89)

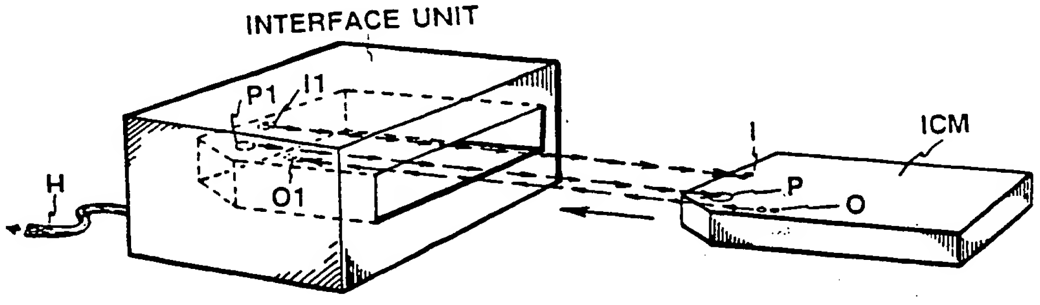
(30) Priority data:
206,001 14 June 1988 (14.06.88) US

(71)(72) Applicant and Inventor: HAIT, John, N. [US/US]; 1836 So. 14th St., Missoula, MT 59801 (US).

(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, KR, LU (European patent), NL (European patent), SE (European patent), SU.

Published
With international search report.
With amended claims.

(54) Title: INDEPENDENT COMPUTER MODULE SYSTEM



(57) Abstract

The device described is a portable, Independent Computer Module (ICM) along with several Interface Units for cc
ing the ICM to a host computer or other external electronic device. The ICM has a CPU, memory, a specialized connec
communication method, a specialized connectorless power supply method, a specialized data and program security memo
sion switching method, all contained in a specialized housing. The ICM with either of the Interface Units constitute an IC
tem which provides multiple advantages as a portable, programmable, secure, safer method of distributing and operating
ter software, an all electronic replacement for floppy disks, and a processor-independent method of using applications pr
with a variety of host computers while providing the ability to parallel process with the host. Modular Interface Units prov
multiple ICMs to be connected to a single host computer, and Remote Interface Units allow multiple ICMs to be acces
host computers from a considerable distance.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australiz
BB	Barbados
BE	Belgium
BF	Burkina Fasso
BG	Bulgaria
BJ	Benin
BR	Brazil
CF	Central African Republic
CG	Congo
CH	Switzerland
CM	Cameroon
DE	Germany, Federal Republic of
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
HU	Hungary
IT	Italy
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
MC	Monaco
MG	Madagascar
ML	Mali
MR	Mauritania
MW	Malawi
NL	Netherlands
NO	Norway
RO	Romania
SD	Sudan
SE	Sweden
SN	Senegal
SU	Soviet Union
TD	Chad
TG	Togo
US	United States of America

Title of the invention: INDEPENDENT COMPUTER MODULE SYSTEM

BACKGROUND OF THE INVENTION

The present invention is related to the safe and secure operation of computer software.

First: A problem arises in the use of software in computers. Typically, the programs to be run are taken from a recording devise such as a disk drive and copied into the Random Access Memory (RAM) of a host computer for processing, or they are programmed into Read Only Memory (ROM) which is either wired directly to the Central Processing Unit (CPU or is encased in a separate module which has a connector for providing direct connection between the CPU and the ROM. The problem is that any user can input a program tha will copy any program that must be loaded into the RAM of a host computer.

Attempts have been made to provide software checks and various security arrangement in an attempt to prevent copying. However, the very nature of the process prevents th institution of effective security measures because, any method that allows the hos computer's CPU to access the program, either by copying it into RAM or directly accessin it in ROM can be copied from that very memory.

In the past, security bank switching arrangements have required complex encryptio equipment, or secret codes for operation. Such methods are expensive, and allow fo corruption by specialized search programs. Such search programs can set up the register in the CPU for loading data from a target program in a target memory bank, and storin data in a common data area or an area of easy access by the search program; then mak multiple jumps throughout the target program until a standard data-moving routine (no corrupted by the new information in the CPU) is encountered. In this way the security c many programs can be violated, programs copied, keys or secret codes can be accessed.

Another method of security violation needs to be addressed. Search programs ofte called "virus" or "worms" hidden in operating systems, unused areas of the host computer memory, or even on diskettes from other sources can write themselves into operating system and into programs being legitimately copied, allowing search programs to compromise t security of anything that passes through that host computer.

Therefore, it became necessary to invent a device that would prevent the direct acce of the host computer's CPU to the program being run, or by any program that could be us by the host computer; thus preventing software copying and theft.

Secondly, the prior art typically uses connectors between program- containing ROM cartridges that must have their power removed to prevent sparking or arcing upon the insertion or removal of the cartridge from its socket. Therefore such methods become unacceptable in certain hazardous environments where explosive gases, or a high percentage of oxygen is present. Even in the normal atmospheric environment such connectors are subject to considerable wear, are difficult to clean, and cause data and program transfer problems.

Certain other environments are hazardous to the computing equipment. Diskettes and disk drives contain delicate mechanical and electrical parts that fail in the presents of dirt or moisture. Thus the prior art does not permit such devices to be used underwater, in outer space, in dirty, chemical-filled, or other hazardous environments.

Third: Prior art software storage devices are incapable of being accessed remotely, or from an environment much different from the normal atmospheric environment.

Fourth: Prior art provides for the distribution of software on diskettes, magnetic tapes or similar devices. The software must be coded for use with a particular CPU, and often for a particular host computer. Therefore a means is needed for software distribution that is both secure, and can operate with a wide variety of host computers regardless of the CPU in the host.

Fifth: Prior art uses mechanical recording devices for programs which are slow, or ROM cartridges which lack the intelligence to be both swift and provide multiple uses.

The present invention solves these problems and provides form many more useful functions.

SUMMARY OF THE INVENTION

The present invention is an Independent Computer Module (hereafter called an ICM) and several types of Interface Units, a generic, a Modular and a Remote. The ICM contains a CPU, ROM and/or RAM memory, a rechargable battery or other energy storage device, a specialized energy supply method, a specialized memory division switching capability, specialized data input and specialized data output method.

The combination of an ICM and one of the Interface Units comprise an ICM System that can function in a multitude of hostile environments, while maintaining strict security over the programs loaded into the ICM. The specialized housing maintains the physical security of the programs inside. The specialized input, output and power supply maintain the electronic security over the programs loaded into the ICM by the fact that the programs themselves do not load into a host computer where they could be compromised, but rather are operated upon by the CPU located within the ICM housing. Program control, and thus all information transfer from the ICM to the host and back are always under the strict control of the CPU and the pre-loaded program within the ICM. Therefore, only data authorized by the ICM program for transmittal will actually be transferred. Such data is transferred to and from the host computer via one of the interface units.

Typically, such data would then be routed by an operating system type program to, or from, any of the peripherals available to the host computer, such as mass data storage devices, CRT video displays, keyboards, printers, etc. Therefore the program inside the ICM can access all of the needed peripherals while maintaining the security of the program, pre-loaded into the ICM. Therefore a separation of function is provided in the present invention. Applications programs are loaded into and operated in the ICM rather than the host, and the host computer is used to operate the usual peripherals. Thus separating the applications program into a separate housing with its separate CPU has provided the opportunity for the secure control of the program that did not exist in the prior art.

Typically, the programs requiring security would be loaded into the ICMs at the time of manufacture, or ICMs manufactured with a minimum, security-controlling prograr operating system would be provided to the software vendor. The software vendor woulc load in the software needing security, and in turn, the ICM would be sold to the end use who would be able to use, but not copy, any of the software.

In order for a host computer to use any number of secure programs, the ICM i constructed inside a portable, conveniently sized housing. When another secure program i to be run, one merely removes the ICM form the interface unit, replacing it witl another...much the same way one would remove a video game cartridge and replace it wit another.

The specialized housing is an integral part of the security arrangement of the ICN system, since the housing is completely sealed, with the programs sealed inside making difficult to mechanically access the secure programs, while the ICMs electrical arrangemer maintains the electronic security.

Further security is provided by the specialized input and output arrangement, as relates to the housing. Input, and output sensors and emitters, along with the power suppl receptors are sealed into the surface of the housing. By sealing in the input and outp arrangement, which is completely controlled by the CPU and its program inside, the housir prevents someone from connecting in a secondary input and output, such as a direct memo access, that could be used to override the other security measures.

The connectorless method chosen for communications and power transfer between tl

Interface Unit (which is connected to the host computer,) and the ICM can be inductive, capacitive, optical or radio frequency emitters, sensors, and receptors. These methods provide the needed data communications and power supply to the ICM while eliminating the need for plugs or connectors, and allowing for remote access to the ICM as they can be sealed into the surface of the housing, and in many cases just under the surface of the housing and still function properly.

For example: If induction is chosen for a particular application, an inductor comprising the primary of a transformer can be mounted in the Interface Unit, and the Secondary of the transformer can be mounted in the ICM. If capacitance is chosen, the metal surface of one side of a capacitor can be mounted in the Interface Unit, and the other surface of the capacitor mounted in the ICM. If optical energy transfer is selected, light emitting diodes (LEDs), phototransistors, and photovoltaics can be used in the ICM and Interface Units. If Radio Frequency is chosen, then RF receivers and transmitters, simple or sophisticated can be used to supply the needed communications and power supply.

Inside the ICM, communications signals to and from the emitters and sensors mounted in the housing are provided to the CPU, while energy from the power-supplying receptor is then rectified (if needed), filtered, and supplied to all powered components including a rechargable battery. Thus the ICM can continue to operate without the need for a plug, or direct connection, is easily removable from the Interface Unit, and will continue to operate for a time after removal from the input power source, so that the ICM can be used to transfer authorized data from one host computer to another.

The Interface Unit need only have a matching set of emitters and sensors, conventional signal matching electronics (if needed) and a direct connection to the host computer and a power source (often from the host computer itself.)

A secondary benefit is derived by so sealing into the housing the input, output, and power supply sensors, emitters and receptors. An environmental seal is maintained, while permitting the communications and energy transference required to operate the internal components. The housing is provided with conventional metallic RF shielding, either on its surface or below surface, and the materials selected for the housing are chosen to operate within an expected hostile environment. For example, an underwater ICM could be completely encapsulated in plastic with the sensors, emitters and receptors encased at or near the surface. While the usefulness of an underwater ICM may not at first seem apparent, the ICM is also immune to coffee, soda pop and other office hazards. Additionally, the ICM could be used in very highly humid environments where the danger of exposure to electronics-damaging items would be a potential possibility such as when computers are in use in submarines, or on board ship.

Another secondary benefit of this communications and power supply arrangement is that the ICM can be inserted and removed from its Interface Unit without causing the arcing that would occur if conventional plugs were in use. This feature makes the use of the ICM especially attractive in potentially explosive environments such as certain industrial environments, in or near equipment used to transfer fuels, or in enriched oxygen environments such as would be common in space stations.

The availability of an additional processor to a host computer, or the availability of a multiple group of ICMs operating from a single host computer provide the opportunity fo parallel processing. Or a user may wish to operate a program using the type of processo that is available within the ICM, but is not available in the host computer. In either case such user programs can be loaded into the ICM and operated by the current user, but suc programs must be prevented from accessing any previously loaded program. Also, occasion may arise whereby the ICM is to be loaded with several secure programs from several user while allowing each user to use each program, but preventing each user from copying an of the previously-loaded programs. Therefore the ICM is fitted with a specialized memor division switching arrangement.

In the internal operation of the ICM, the Central Processing Unit (CPU), program-fille Read Only Memory (ROM), Random Access Memory (RAM), and the specialized input an output, and power supply sections inside the ICM constitute a complete computer that ca operate programs loaded into memory in the standard fashion. All of this memory divided into sections and division switched by a specialized division switching arrangeme that prevents the programs in one division from accessing the programs in any oth division. One section of memory is designated as a Common Area and is memory mapp so that it is available to all divisions. The division switched sections of memory are divide into two types, the Executive Division (EXEC) and the Selected Divisions. The Executi Division has complete control and access to all other areas for security and controlli transfer of data between Divisions. The Selected memory Divisions are provided for us programs, and are restricted so that user programs with in a Selected Division cannot co directly any data from any other Division (except the Common data storage Area).

A division switching apparatus is provided that causes the Executive Division to operative after a reset of the CPU. The division switching apparatus is connected to t control bus so that commands taken from the Executive Division can cause both reads a writes of data in any memory division, while fetching its instructions from the Executi Division only. Also a means is provided for transferring program control to any of t other divisions either directly, or with an accompanying maskable or non- maska interrupt.

The Selected Divisions, on the other hand, have the capability of fetching, reading a writing to its own division, and the Common Area only. Transfer of program control, to any other division is always accompanied by a non-maskable interrupt (NMI), which causes a hardware interrupt, and program control to a designated place in the newly-switched-on memory. (Or if a maskable interrupt is used, the division switching is prevented unless an interrupt acknowledge signal is received from the CPU indicating that an interrupt is actually in progress, thus preventing the execution of a division switch without an accompanying interrupt.) These designated entry points are programmed to be operating system entry points, so that information exchange between the divisions is always controllable. This method even allows the loading of any outside program while maintaining the security of the programs in the other memory divisions. By using the NMI, no program (except the executive program contained within its own division) could seek to find normal data transfer routines in a different target division and corrupt these through adjustments in CPU register values in and attempt to move private data into the Common Area by entering the target program at non-standard points looking for normal data movement routines.

The result is that the individual programs loaded into each of the Selected Divisions can be loaded directly into Programmable Read Only Memories (PROMs), Erasable Read Only Memories (EPROMs), or even RAM, but are still unable to copy any information from any of the other divisions, but any needed data can be provided by the program in the Executive bank. The host computer may, at the discretion of the program in the ICM Executive, load programs into the ICM for operation, in any of the Selected Divisions. The host may receive input and output from those programs. However, the Executive program can effectively prevent any outside loaded program form copying any data that the Executive does not permit, even though each of the programs may have direct access to the ICM input and output to the host. Permanently stored programs can thus be accessed and used at any time by inserting the ICM into an Interface Unit, or accessing it with a Remote Interface Unit. The ICM can accept outside programs, even temporary ones loaded into the ICM RAM, without compromising the previously stored programs.

Individual memory divisions are selected, usually by means of a decoder, or a ROM used as a decoder and signal director, on the basis of four input codes. The first code is the Division Selection code which is loaded into a code storage device upon command from the CPU. The second code is the Mode Select code, also loaded into a code storage device upon command from the CPU. The third is the Address Bus, for memory mapping the Common Data Area. The fourth is the Control Bus.

By selecting the individual memory divisions based on all four codes, both the security arrangement that results from Mode and Selected Division codes, and the ability to more rapidly copy data from one division to another by the Executive program is produced. The security arrangement, is, in part, functional because the Executive Division is switched on by a selection of a mode rather than the selection of a Selected division, (which is the prior art way.) Since the Executive Division is part of the mode selection, any other memory may be accessed by the Executive Division simply by changing the Selected Division code.

The selection of a mode that causes command fetches to come from the Executive Division, and reads and writes to be operative on other divisions allows the Executive program to use fewer CPU commands to move data from one division to another, by using a standard move routine as would be used within a single division, but causing the reads to come from one division and the writes to another. This feature is especially useful when the Executive program is working as an operating system to shuttle information back anc forth between an applications program and the host computer.

The ICM housing is also fitted with a physical damage security system consisting of a damage sensor made of a maze of wires located just under the surface of the housing Attached to these wires is a method for measuring the wire's resistance, which, in turn, i connected to the CPU. Also connected to the CPU is a self-destruct mechanism, of an convenient kind, that is capable of destroying the memory sections of the ICM. In the even that someone should try to either cut into the ICM, and thus through the wires or try t defeat this security mechanism by shorting it out, the CPU would sense the change i resistance, and would then activate the self- destruct mechanism.

Interface Unit: The ICM is interfaced with a host computer or other electronic devic through a specialized Interface Unit. This unit also has a specialized housing that completely sealed to prevent damage to the components from a hostile environment. It provided with a port, or other device for holding the ICM so that its sensors, emitters an receptors are adjacent to corresponding emitters and sensors in the Interface Unit. Th Interface Unit is fitted with a cable or similar wiring for connecting it directly to a ho computer. Room is provided in the housing for any interfacing circuitry needed to opera the sensors and emitters, and connect them properly to the host.

A specialized Modular Interface Unit (MIU) is provided. The MIU has all of t features of a generic Interface Unit, but is also fitted with two connectors, front and bac so that a number of interface units may be connected together to be operated by a sing host computer.

A Remote Interface Unit (RIU) is also provided. The ICM can also be interfaced wi a host computer through a specialized interface unit that can operate over a longer distan than would be usual with the generic or modular interface units. The RIU has emitters, a sensors selected for the range and type of communications and power to be supplied. F example, the RIU may have infrared LEDs and phototransistors for communicating with t ICM, or several ICMs at a time from across the room. Whereas, modulated lasers a focusing collectors may be required to communicate with an ICM at a considerable distance or in a different hostile environment such as under the sea. The types needed for a particular task are simply chosen and installed during manufacture. The RIU housing may also be sealed for operation in a hostile environment, and is fitted with cables, and interfacing electronics just as any of the Interface Units would be. Remote interfacing of the ICMs with a host computer allows for the multiple access of many ICMs by the same Remote Interface Unit, while allowing ICMs made for use in one hostile environment to be accessed by a RIU and host in a different environment. This remote capability also allows several users with separate hosts and RIUs to use common ICMs while still maintaining security of the programs.

The versatility of the ICM System makes it a safer, applications- program-running, processor-independent, remotely-accessible, parallel- processing, hostile-environment-proof, completely-secure, all-electronic, replacement for the conventional floppy disk.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1. An exterior exploded perspective view of the Independent Computer Module (ICM) and a generic Interface Unit showing the relationships of inputs and outputs.

Figure 2. A cross section view of a Modular Interface Unit (MIU) with an ICM inserted, and showing the positions of additional MIUs if used.

Figure 3. A perspective view of an ICM being accessed by a Remote Interface Unit (RIU).

Figure 4. A detailed block diagram of an ICM and an Interface Unit, showing the memory division switching method, the specialized input, output and energy supply method, along with the mechanical access security system.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Figure 1 depicts an exploded perspective of the ICM being inserted into a generic INTERFACE UNIT. The ICM is contained in its specialized housing that is completely sealed using materials selected for protection in the particular environment that it is intended to be used. For example, to make the ICM useable underwater, it could be completely encapsulated in plastic.

In operation, the ICM is inserted into the INTERFACE UNIT for connecting the ICM to a host computer through wire H. Input power, and data communications are accomplished through a connectorless energy and data transfer arrangement using sensors, emitters, and receptors I1,I,O1,O,P1,and P. The ICM is held in place by the INTERFACE UNIT, so that the respective emitters are held adjacent to their counterpart sensors etc.

Input power to the ICM for recharging its batteries is provided from the host through an emitter, P1, which transfers energy to receptor, P. Data communications is provided through an input and an output set of emitter/ sensor pairs I1 and I for the input to the ICM, along with O1 and O for the output. A sufficient number of emitter/sensor sets is provided to accommodate all the data and handshaking signals of a standard serial or parallel data port. The type of emitter/sensor pair is selected to match the type of energy transfer needed for a particular application with one of each pair in the INTERFACE UNIT and the other in the ICM.

For example: for connectorless induction data and energy transfer, the primary portion of a split transformer (manufactured in two mechanically separate sections) would be located in one unit and the secondary portion in the other. For capacitive connectorless energy and data transfer, one capacitive surface of a split capacitor (also manufactured in two mechanically separate sections) would be located in one unit and the matching capacitive surface in the other. For optical connectorless energy transfer a light sourc would be provided in the INTERFACE UNIT for power, and photovoltaic cells in the ICM, while data transfer could be by light emitting diodes (LEDs) and phototransistors. For radi frequency energy and data transfer the emitter would be a radio transmitter, and the senso or receptor would be a radio receiver.

These emitters, sensors and receptors are sealed into the surface, or just under th surface of the ICM housing so they can operate normally while maintaining the hazardou environment protection. The INTERFACE UNIT, likewise can be sealed with the senso and emitters sealed into the interior surface of the Interface Unit housing.

Figure 2 depicts a cross section of a Modular Interface Unit, MIU, having a por PORT, for holding the ICM so that its emitters, sensors and receptor are held adjacent a matching set of emitters and sensors (P1 near P, I1 near I, and O1 near O) for supplyi power and communications to the ICM. Just as describe for Fig. 1.

The Modular Interface Unit has the additional feature of connectors C1 on one side a C2 of the other side. These connectors allow the addition of more Modular Interface Un MIU1 and MIU2 (dotted lines) so that a number of ICMs can be operated by a single h computer. Wire and connector H is the connecting wires to the host computer that m come from at least one of the MIUs. A seal, S, is provided to prevent damage to t connectors C1 and C2 from a hostile environment. Standard interface electronics, mounted on a conventional printed circuit board, is provided to connect the emitters a sensors to the host.

Figure 3 depicts an ICM being accessed and operated through a Remote Interface U RIU. The RIU has input (to the ICM) emitters I1 and output (from the ICM) sensors

Power output (to the ICM) emitter P1 along with the connecting wires to the host. Just as described in Fig. 1. Emitters and sensors in the RIU are positioned so as to be directed toward the ICM. The RIU housing is also tightly sealed and made of selected materials so that it may be used in a hostile environment, possibly a different environment from the environment that the ICM is operating in.

All of the Interface Units function exactly alike; they serve to provide an connectorless interface between a host and one or more ICMs. The different types are provided to give greater versatility to the operation of the basic ICM System.

Figure 4 is a block diagram of a typical ICM and an Interface Unit. Energy is supplied from the host computer through wires,H, and standard interface electronics IE1, through the power emitters P1 of the Interface Unit (any of the types) to the power receptors P in the ICM.

Sensors and emitters are fitted with a hazardous-environment-safe energy conductor, EC. EC is a material selected to provide hazardous environment protection to the component while permitting the energy form in use for power and data transfer to pass through. For example, clear plastic or fiber optics would be provided to pass light from an emitter to the surface of one unit, then from the surface of the other unit to the sensor inside, if the emitters and sensors are optical. Or a thin plastic cover could be provided to pass energy using induction, capacitive, or radio transfer, depending on the expected hazardous environment to be encountered.

ICM input power from P is rectified (if needed) and filtered in the power supply section PWR, and then distributed to all powered components in the ICM (labeled TO ALL) plus the rechargable battery B.

Data input and output from the host computer is supplied through wires, H, and standard interfacing electronics IE2 to the emitters and sensors I1 and O1 of the Interface Unit to the matching emitters and sensors I and O in the ICM. These are in turn connected through a standard input/output interface, I/O, to the CPU.

This arrangement of emitters, sensors, and receptors provide connectorless communications and power supply between the host and the ICM.

Output (or memory mapped) mode, memory division selection, and switching commands are decoded by Read Only Memory ROM1 (or a similar arrangement of AND and OR functions) with outputs to strobe each of the components individually or simultaneously as needed to carry out each command. Non-Executive Division Select Latch and Mode Select Latch store the division selection and mode codes output from the CPU upon receiving a strobe from ROM1. ROM2 decodes the address, control, mode, and division select signals to provide the instantaneous division selection required among the memory divisions designated as: The Executive Division, EXEC; the Common Data Division, Com; and individually Selected Divisions Mem 1 through Mem n.

ROM1 also has an input feed back line, FB, taken from the output of the Mode Select Latch. This line is on or off depending on whether the Executive memory division is currently in program control or not. This line determines the modes that will be permitted to be loaded depending upon the memory division which has program control. It is this line that provides the ICM with the ability to provide a secure operating system in the EXEC Division while preventing programs in the other divisions from instituting modes that would allow unauthorized data copying; along with the fact that the EXEC Division is not selected as one of the Selected Divisions, but its selection is one of the Modes.

ROM1 also has an output to the CPU non-maskable interrupt, NMI. When FB indicates that a Selected Division has program control, all division switching commands provide a simultaneous NMI. This is also an important part of the security arrangement, because thi line prevents a search program from switching program control to a target division whil entering at various places in the target program (as could occur in a conventional ban switching arrangement,) in an effort to discover a routine that could be misused to provid unauthorized data. The NMI causes program control to begin at a set address in the targe division; if programmed as a special program, or operating system entry point, the targe program will be able to prevent an attempted corruption of any of its routines b initializing the CPU registers, as it needs, to protect its data movement routines.

ROM1 is also programmed to allow the simultaneous loading of a mode 0 while causin an NMI. This command is permitted whenever FB indicates that the Selected Divisions ha program control. This command is used to switch to the Executive program whenev operating system type functions are desired. By choosing the best fetch/read/wri functions to take place within a given CPU command sequence for mode 0, the most rap transfer of data can be accomplished by the Executive program.

ROM1 also has an output connected to the CPU maskable interrupt, INTR. This li is operative only when the EXEC Division has program control, as indicated by line F Maskable interrupts (depending upon the CPU chosen) often have a software programmat interrupt entry point. If available, this would make the Executive program much m versatile. Otherwise, the Executive program can select the program control beginni address in a Selected Division by simply changing modes from a position in the Comm Data Division, and jumping to the desired starting point. Selected divisions would prohibited from doing this by FB, ROM1 and the NMI.

The Mode Select Latch is CLEARed by the RESET signal from the CPU, the EXEC Division is designated by ROM1 as having program control in mode 0. Therefore, upon receiving a reset signal, mode 0 is selected, so the EXEC Division has initial program control.

ROM2 decodes the four major codes, the Division Select code, the Mode Select code, the ADDRES BUS code, and the CONTROL BUS code to provide the selection of memory divisions that produce the the following fetching, reading and writing sequences based on the following modes:

0 Fetch from EXEC -- Read and Write to Selected Division
1 Fetch and Read from EXEC -- Write to Selected Division
2 Fetch from and Write to EXEC -- Read from Select Division
3 Fetch & Read from, Write to EXEC
4 Fetch & Read from, Write to Selected Division

Also: the Common memory Com is memory mapped by ROM2 into an address space accessible from all memories, while other required memory operational signals will also be timed and provided properly, such as refresh for dynamic RAMs.

ROM1 is specially programmed to provide the following command decoding and control functions:

When FB indicates that the EXEC Division is NOT in use:

1. Load 0 into Mode Select Latch, and produce an NMI.
2. Load Division Select Latch, Load code for mode 4 into Mode Select Latch and cause an NMI.

When FB indicates that the EXEC Division IS in use:

1. Load Division Select Latch
2. Load Mode Select Latch.
3. Load Mode Select Latch, and cause a Maskable Interrupt, INTR

A physical entry security system is also provided. A maze of wires (labeled MAZE) is located just under the surface of the entire ICM housing. These wires are connected to a resistance detector, DET., which, in turn, is connected as an input to the CPU. DEST. is a self destruct mechanism located so as to be able to destroy the memory divisions if activated by the output from the CPU. If a cut is made in the housing, of if someone attempts to defeat this security device by shorting out the wires, the resistance detector will indicate the change in resistance to the CPU which can then activate the self destruct mechanism to prevent the information stored in them from being accessed.

CLAIMS

What is Claimed is:

CLAIM 1: An Independent Computer Module System composed of an Independent Computer Module (hereafter referred to as an "ICM"), and an Interface Unit, for connecting said ICM to a host computer or other electronic device.

Said ICM containing a computer comprised of, at least, a central data processing means, a data storage means, a rechargable energy storage means, a data communications and energy supply means all contained in a single portable housing.

Said interface unit having means for transferring energy to said ICM, a means for providing data communications with said ICM, and a direct electrical connection to a host computer or other electronic device. Said Interface Unit having a means for the quick and convenient connection and disconnection between said Interface Unit and said ICM.

The present invention constitutes an improvement over the prior art in that a separatior is made between the host computer with its non-secure memory and the operation of the applications program (either completely or in part) within said secure ICM. Saic applications programs can access all of the available host peripherals including any mas data storage device that may be available, by means of said communications means, througl said host computer, while maintaining the security of programs loaded into said ICM. Sai central processing means, within said ICM, operating said applications programs within sai ICM also maintains program control such that all data transfer into or out of said housin to said host computer can be controlled so that no outside, unauthorized program may b loaded into said ICM in an attempt to remove secure data.

The present invention is an improvement over the prior. art in that an applicatio program need only be written to operate on said central processor within said ICM. Sinc the programming within said host need only be of the operating system type with a dat communications capability between said host and said ICM. Therefore, said applicatio programs become host-processor independent, and can be operated using any number of ho computer types without changing said applications program.

The present invention is an improvement over the prior art in that a second centr processing means has been added to assist applications programs to operate quicker and wi the expanded capabilities of processing in parallel using both said host and said IC computers simultaneously.

The present invention is an improvement over prior art in that said ICM with sa secure applications programs can load and store data from said host computer. Then sa ICM may be transferred to another host computer, then in turn, said data may transferred to said second host. Therefore, said ICM System constitutes an all electronic replacement for the present floppy drives and diskette software distribution and data storage method.

CLAIM 2: An ICM System as described in Claim 1 having a connectorless communications means for providing two-way data communications between said ICM and said host equipment through said Interface Unit. Said Interface Unit having standard interface devices for connecting said connectorless communications means and said host equipment.

CLAIM 3: An ICM System as described in Claim 2 having split transformer connectorless inductive communications means between said ICM and said Interface Unit. Said split transformers each having at least two windings, one located in said Interface Unit with half of said transformer's core and the other winding located in said ICM with the other half of said transformer's core. Said ICM System having as many of said split transformers as are needed to pass all required data communications signals between said ICM and said Interface Unit. Said split transformer being positioned in said ICM housing, and said Interface Unit such that said split transformer parts are near enough to each other to provide useful inductive communications.

Said split transformer, inductive, connectorless data communications means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

CLAIM 4: An ICM System as described in Claim 2 having a split capacitor connectorless two-way communications means between said ICM and said Interface Unit. Said split capacitors having one capacitive surface located in said ICM housing and the other capacitive surface located in said Interface Unit and located such that said communications signals may pass between said ICM and said Interface Unit by capacitive action. Said ICM System having a sufficient number of split capacitors to pass all of the necessary communications signals between said ICM and said Interface Unit.

Said capacitive connectorless data communications means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

CLAIM 5: An ICM System as described in Claim 2 having a sufficient number of matched sets of optical emitters and sensors in said Interface Unit and said ICM connected so as tc provide two-way connectorless communications between said ICM and said Interface Unit.

Said Optical connectorless data communications means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

Said optical connectorless data communications means is an improvement in that said ICM may be accessed directly by a number of host computers, and from a further distance than direct wiring, or insertion directly into an Interface Unit would allow.

CLAIM 6: An ICM System as described in Claim 2 having a two-way radio frequency data communication means between said ICM and said Interface Unit.

Said radio frequency connectorless data communications means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

Said radio frequency connectorless data communications means is an improvement in that said ICM may be accessed directly by a number of host computers, and from a further distance than direct wiring, or insertion directly into an Interface Unit would allow.

CLAIM 7: An ICM System as described in Claim 2 having a connectorless means fo transferring energy for electrical power to said ICM from said host equipment, through saic Interface Unit. Said Interface Unit having standard interface devices for connecting sai connectorless energy transfer means and said host equipment.

Said connectorless energy transfer means and said connectorless communications mean are an improvement in that an ICM may be removed from and inserted into an Interfac Unit many times without causing the problems that come from worn or dirty connectors

CLAIM 8: An ICM System as described in Claim 7 having split transformer connectorle energy transfer means between said ICM and said Interface Unit. Said split transforme each having at least two windings, one located in said Interface Unit with half of sa transformer's core and the other winding located in said ICM with the other half of sa transformer's core. Said split transformer being positioned in said ICM housing, and sa Interface Unit such that said split transformer parts are near enough to each other provide sufficient inductive energy to power said ICM.

Said split transformer, inductive, connectorless energy transfer means is an improvement in that said ICM may be connected to, and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

CLAIM 9: An ICM System as described in Claim 7 having a split capacitor connectorless energy transfer means between said ICM and said Interface Unit. Said split capacitors having at least one capacitive surface located in said ICM housing and at least one other capacitive surface located in said Interface Unit and located such that said powering energy may pass between said ICM and said Interface Unit by capacitive action.

Said capacitive connectorless energy transfer means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

CLAIM 10: An ICM System as described in Claim 7 having an optical emitter in said Interface Unit and a photovoltaic device in said ICM for transferring energy to power said ICM from said Interface Unit.

Said Optical connectorless energy transfer means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

Said optical connectorless energy transfer means is an improvement in that said ICM may be powered directly by a host computer at a further distance than direct wiring, or insertion directly into an Interface Unit would allow.

CLAIM 11: An ICM System as described in Claim 7 having a radio frequency energy transfer means to said ICM from said Interface Unit for providing electrical power to said ICM.

Said radio frequency connectorless energy transfer means is an improvement in that said ICM may be connected to and disconnected from said Interface Unit, and thus to and from said host equipment, while said ICM is still operating, without arcing or causing a spark that might cause a fire, cause radio interference, or detonate an explosive atmosphere the ICM may be operating in.

Said radio frequency connectorless energy transfer means is an improvement in that said ICM may be powered by a host computer from a further distance than direct wiring, or insertion directly into an Interface Unit would allow.

CLAIM 12: An ICM System as described in Claim 7 having a specialized ICM housing. Said ICM being housed inside a specialized portable housing, of any convenient shape to allow said ICM to be positioned for proper interaction with said Interface Unit. Said housing being completely sealed with materials selected so as to protect the internal components from damage from hostile environments, with said materials being particularly chosen to function in said expected hostile environment. Said specialized housing having energy input receptors, and data communications sensors and emitters sealed into said housing and located so as to match the respective positions of the counterpart emitters and sensors in said Interface Unit.

Said housing having a means for allowing the flow of the respective energy forms from the surface of said ICM to said receptors, sensors, and emitters.

Said housing is an improvement in that said ICM would be portable, useable in hostile environments, and would facilitate the operation of all of the various features of said ICM System.

Said housing is an improvement in that a completely sealed housing can be made more difficult to open mechanically in an attempt to access secure memories and thus said housing enhances the security of said ICM System.

CLAIM 13: An ICM System as described in Claim 12 having contained within said ICM housing a mechanical access security system. Said security system having a means for sensing an attempt to cut, drill, or otherwise break into said housing. Said security system having a means to destroy the contents of all secure memories within said ICM upon ar attempted mechanical access. Said security system is an improvement in that it would make mechanical access even more difficult.

CLAIM 14: An ICM System as described in Claim 7 having a specialized Interface Unit Said Interface Unit having a specialized housing that is completely sealed with material selected so as to protect the internal components form hostile environments. Said Interfac Unit having said communications and energy supply emitters and sensors sealed into sai Interface Unit housing with energy conductors, a means for allowing the flow of respectiv energy forms from the surface of said housing to said emitters and sensors. Said Interfac Unit having at least one holding device for holding said ICM into place with respect to th entrances and exits of said energy conductors in said housing, in order to provide the prope functioning relationship between said Interface Unit and said emitters, sensors and recepto in said ICM.

CLAIM 15: An Interface Unit as described in Claim 14 being made modular in nature, being provided with connectors on opposite sides of the Interface Unit module to accommodate the additional connection of more Modular Interface Units so that a number of ICM interfaces may be connected to a common host computer or other electronic equipment. Said Modular Interface Unit having a seal around said external connectors to protect said connectors from said hostile environment.

CLAIM 16: An Interface Unit as described in Claim 14 having the ability to access a number of ICM units remotely, constituting a Remote Interface Unit. Said Remote Interface Unit having its ICM counterpart emitters and sensors arranged for proper transfer of energy and data communications in a functioning relationship with said ICM emitters and sensors in a remote position.

CLAIM 17: An ICM as described in Claim 1 having a specialized memory division switching means. Said ICM containing a memory means that can be divided into separate divisions. Said memory divisions having one such memory division designated as the "Executive Division", and the remainder designated as "Selected Divisions."

Said division switching means having: output signals under program control from said central processor; data storage devices for storing mode select and division select information; a means for controlling output command signals based on the contents of said mode select storage device; and a means for selecting individual memory divisions based on fetch, read, write, refresh information signals from said central processor in addition to said stored mode and division select information. Said memory division selection also being accomplished whenever said refresh signal is present, in order to refresh all memories that are of the Dynamic RAM type.

Said modes selected produce all the possibilities of combinations for fetching instructions, reading data, and writing data to and from all said memory divisions. Said modes include:

1. Fetch from Executive Division; read from and write to Selected Division.
2. Fetch and read from Executive Division; write to Selected Division.
3. Fetch from and write to Executive Division; read from Selected Division.
4. Fetch and read from, and write to Executive Division.
5. Fetch and read from, and write to Selected Division.

Said program controlled output signals having the following command functions operable ONLY when said mode select information indicates that said Executive Division is in program control, in that fetch instructions, as determined by the current mode, would be directed to said Executive Division:

1. Load Selected Division storage means.

2. Load Mode Select storage means.

3. Load Mode Select storage means, and cause an interrupt to said Central Processor such that program control begins at a pre-determined address.

Said program controlled output signals having the following command functions operable when said Executive Division is NOT in program control, that is, when fetch instructions, as determined by the current mode, would not be directed to said Executive Division:

1. Load Selected Division storage means, and cause a non-maskable interrupt and a change in program control to a predetermined, hard wired, program address.

2. Load Mode Select storage means with an Executive Division fetch mode code, and cause a non-maskable interrupt and a change in program control to a predetermined, hard wired, program address.

3. Cause a maskable interrupt and thus a change in program control to a predetermined, hard wired, program address. Then load Mode Select storage means with an Executive Division fetch mode code only upon the receipt of an interrupt acknowledge signal fron said Central Processor.

4. Cause a maskable interrupt and thus a change in program control to a predetermined hard wired, program address. Then load said Selected Division storage means only upon th receipt of an interrupt acknowledge signal from said Central Processor.

Said memory division switching means is an improvement in that programs in sai Selected Division memories are secure from each other because program control canno transfer from one Selected Division to another without causing a simultaneous change i program control address to a hard wired address in the newly-switched-in memory divisio thus no program in any of the memory divisions can copy information from any othe memory division. However the program located in said Executive Division can control th movement of data to and from all memory divisions.

Said memory division switching means is an improvement in that user programs ma be loaded into said ICM and executed with different programs in separate divisions, eve from different users, while maintaining the security of each program both within said IC and between each division.

Said memory division switching means is an improvement in that it establishes parallel memory arrangement whereby programs within said Executive Division may re and write data anywhere in a Selected Division even if the position in said Select Division has the same address as is occupied by the program in said Executive Divisic Thus data may be transferred much more rapidly to and from two separate divisions means of single program commands to said Central Processor without the need for switching divisions back and forth with division switching commands but just as if the transfer were taking place within a single division.

CLAIM 18: An ICM as described in Claim 17 having a separate memory division designated as the "Common Data Area". Said Common Data Area is memory mapped such that it is automatically addressable as a part of all divisions. Said memory map is arranged such that said interrupt, hard wired, program entry points are not a part of said Common Data Area.

The addition of said Common Data Area is an improvement in that all programs in each of said Selected Divisions can access said Common Data Area, however security between said Selected Divisions is maintained because any switching from one Selected Division to another is always accompanied by an interrupt and a change in program control to a predetermined location in the newly-switched-in division, thus all program control is maintained within any target program which can thus control all information transfer, while providing a rapid means of transferring authorized data from one Selected Division to another.

CLAIM 19: An ICM as described in Claim 18 having a means for programming those memory divisions constructed with Programmable Read Only Memories, and other non-volatile memory divisions. This is an improvement in that power may be removed from said ICM for a considerable time while maintaining user programs and the security of said programs.

AMENDED CLAIMS

[received by the International Bureau on 21 November 1989 (21.11.89)
original claims 1-19 replaced by amended claims 1-15 (2 pages)]

1. A secure computer architectural and apparatus system comprised of an Independent Computer Module (here after referred to as an ICM), and an Interface Unit, for connecting said ICM to a host computer;

said ICM comprising a computer having a central data processing means, a memory means, a two-way data communications means, and an energy supply means, all contained in a single cartridge housing;

said communications means being controlled by command-signals from said processing means for the purpose of transferring data into and out of said ICM;

said Interface Unit comprising a means for transferring energy to said ICM, a means for two-way data communications with said ICM, a connection means for two-way data communications with said host computer, and a means for holding said ICM cartridge in a working position with respect to said data communications and energy supply means.

2. A computer system as claimed in Claim 1 further comprising a connectorless interface means for providing two-way communications as a part of the said communications means inside said ICM cartridge, and a connectorless means for providing two-way communications as the said communications means within said Interface Unit.

3. A computer system as claimed in Claim 2 further comprising inductors as the said connectorless communications means having an inductor means located within said ICM, and an inductor means located within said Interface Unit.

4. A computer system as claimed in Claim 2 further comprising electrical capacitors as the said connectorless communications means having one plate of each said capacitor in said ICM, and one other plate of each said capacitor in said Interface Unit.

5. A computer system as claimed in Claim 2 further comprising, as the said connectorless communications means, optical emitters and optical sensors.

6. A computer system as claimed in Claim 2 further comprising, as the said connectorless communications means, radio frequency transmitters and radio frequency receivers.

7. A computer system as claimed in Claim 2 further comprising a connectorless interface means for supplying electrical energy to power said ICM.

8. A computer system as claimed in Claim 7 further comprising an inductive connectorless means as the said connectorless means for supplying electrical energy to power said ICM, having an inductor located within said ICM, and an inductor located within said Interface Unit.

9. A computer system as claimed in Claim 7 further comprising a capacitive connectorless means as the said connectorless means for supplying electrical energy to power said ICM, having one plate of an electrical capacitor in said ICM, and one other plate of said capacitor in said Interface Unit.

10. A computer system as claimed in Claim 7 further comprising an optical means as the said connectorless means for supplying electrical energy to power said ICM.

11. A computer system as claimed in Claim 7 further comprising a radio frequency means as the said connectorless means for supplying electrical energy to power said ICM.

12. A computer system as claimed in Claim 7 further comprising a sealed cartridge so as to prevent damage to internal components by environmental factors.

13. A computer system as claimed in Claim 7 further comprising a sealed housing, for said Interface Unit so as to prevent damage to internal components by environmental factors.

14. A computer system as claimed in Claim 1 further comprising said memory means being divided into two independently addressable memory subdivisions comprised of:

(a) Said first memory subdivision comprising non-volatile read-only type memory as one portion of the addressable range of said first memory subdivision to prevent alteration of information contained therein;

(b) Said second memory subdivision comprising read/write random access type memory as one portion of the addressable range of said second memory subdivision to permit the alteration of information contained therein.

15. A computer system as claimed in Claim 14 further comprising a memory subdivision switching means for controlling read/write access to said first memory subdivision by said processing means, upon receiving command-signals from said processor;

said switching means comprising:

(a) a means of turning off said access to said first memory subdivision upon said switching means receiving a command-signal from said processor;

(b) a means for turning on said access to said first memory subdivision upon said switching means receiving a command-signal from said processor, which simultaneously causes a non-maskable software command control jump to a fixed address within said first memory subdivision;

(c) said switching means having a latching means for maintaining the off and on states of said switching means between said command-signals.

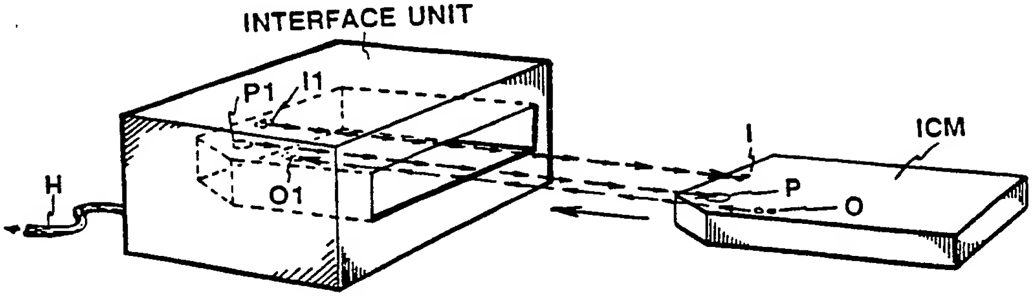

INTERFACE UNIT
P1
I1
O1
H
I
ICM
P
O

FIG. 1

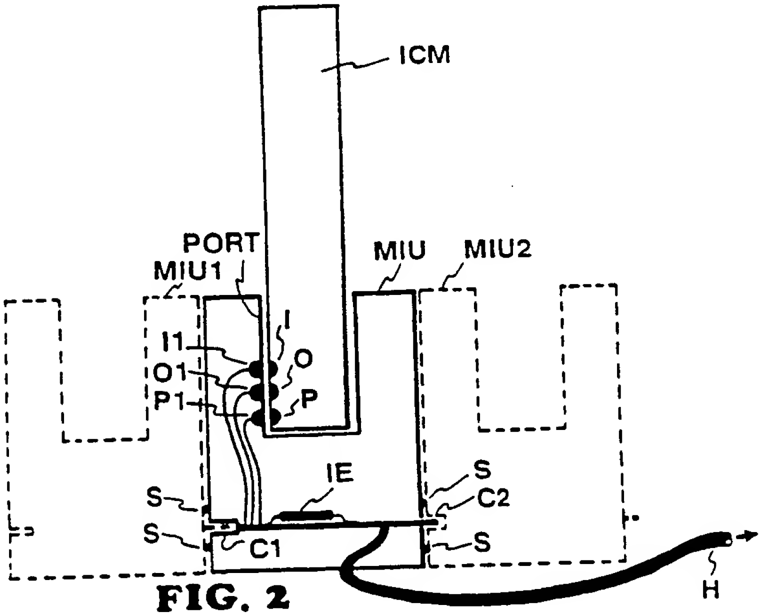

ICM
PORT
MIU1
MIU
MIU2
I1
O1
P1
I
O
P
IE
S
S
S
C2
S
C1
H

FIG. 2

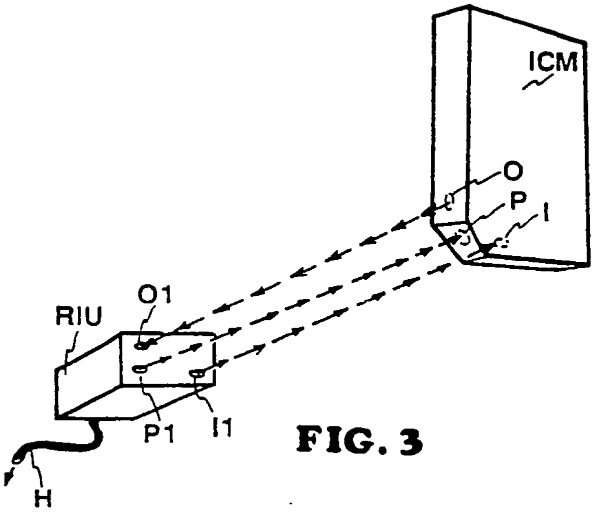


FIG. 3

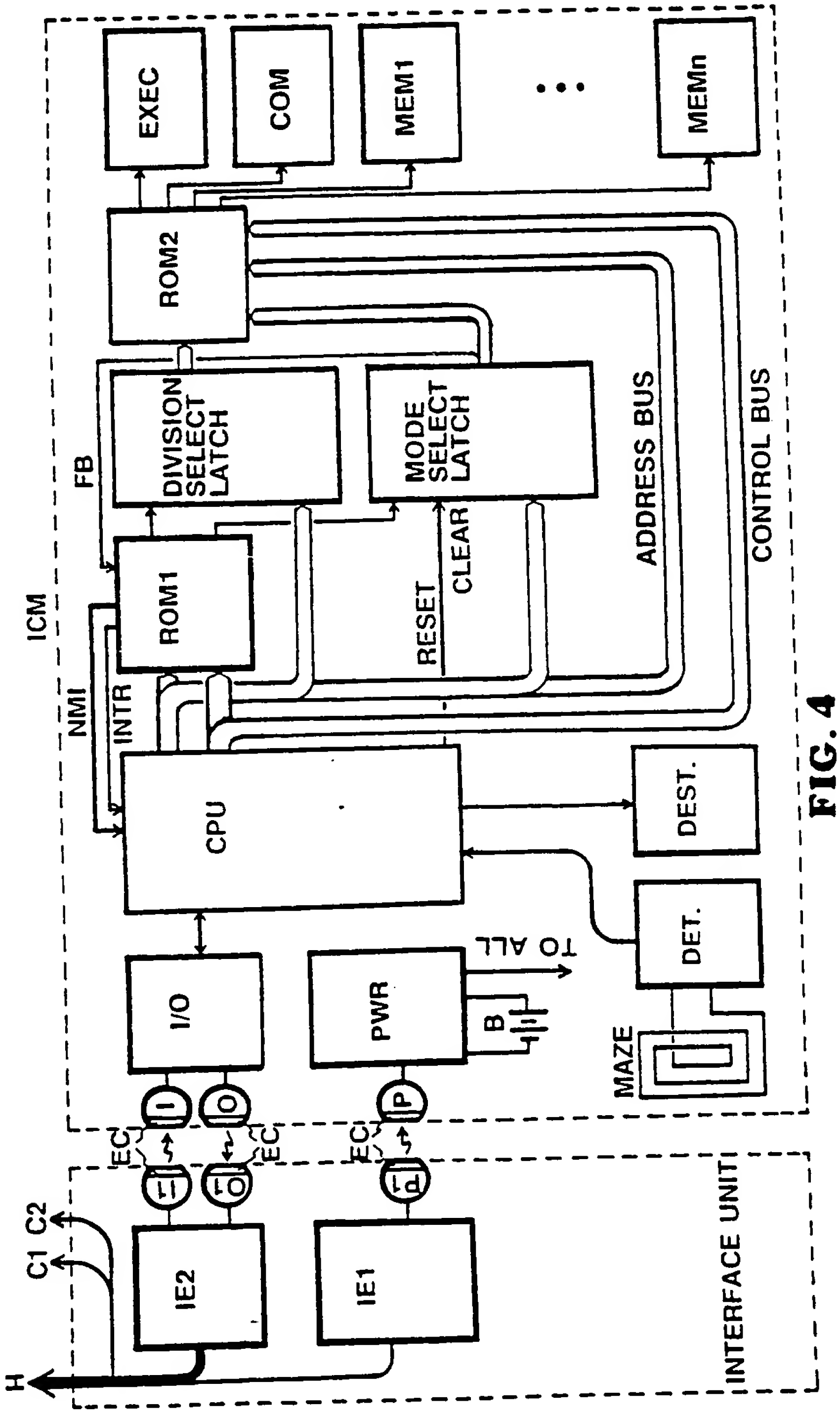

ICM
EXEC
COM
MEM1
• • •
MEMn
ROM2
DIVISION SELECT LATCH
MODE SELECT LATCH
FB
ROM1
NMI
INTR
RESET
CLEAR
ADDRESS BUS
CONTROL BUS
CPU
DEST.
DET.
MAZE
I/O
PWR
B
TO ALL
I
O
P
EC
EC
EC
I1
O1
P1
IE2
IE1
C1
C2
H
INTERFACE UNIT

FIG. 4

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US89/02360

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(4): G06F 12/14, 13/00
U.S. CL. 364/200, 300

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
U.S.	364/200, 300

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	US, A, 4,521,853 (GUTTAG) 06 JUNE 1985	1-19
A	US, A, 4,328,542 (ANASTAS et al.) 04 MAY 1982	1-19
A	US, A, 4,652,990 (PAILEN et al.) 24 MARCH 1987	1-19

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search 15 AUGUST 1989	Date of Mailing of this International Search Report 28 SEP 1989
International Searching Authority ISA/US	Signature of Authorized Officer Eddie P. Chan EDDIE P. CHAN